Legal Evaluation of FutureID

Deliverable 12.7

Document Identification	
Date	30/10/2015
Status	final
Version	Version 1.0

Related SP / WP	SP1 / WP12	**Document Reference**	D12.7
Related Deliverable(s)	D22.6, D32.8, D51.5, D52.5	**Dissemination Level**	PU
Lead Participant	KUL	**Lead Author**	Jessica Schroers
Contributors	Hannah Obersteller (ULD)	**Reviewers**	Jon Shamah (EEMA) Detlef Houdeau (IFAG)

This document is issued within the frame and for the purpose of the FutureID project. This project has received funding from the European Unions Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 318424

1. Abstract

In this deliverable the three artefacts (reference architecture, implementation and pilots) are evaluated on the basis of the legal requirements as stated in D22.6. The Design Science Methodology framework has been used, as it is the common evaluation approach for the FutureID evaluations across multiple disciplines. For the legal evaluation, many requirements were considered not applicable for the specific artefacts. Therefore, an additional section was added which considered a possible deployment scenario based on one of the pilots.

For the reference architecture artefact, almost none of the requirements were applicable. For the implementation artefact, some requirements were applicable. All applicable requirements have been considered as passed since the implementation allows a legally compliant deployment. However, the passing of a requirement on an implementation level does not automatically mean legal compliance of the deployment, only that it is technically possible to deploy the system legally compliant.

Accordingly, for a legal evaluation, the final deployment is the important part, which could however not be evaluated as the final deployment is not yet realized. For this reason, and due to the fact that most requirements for the pilots were not applicable as no personal data was used, a scenario involving the e-learning pilot, assuming that personal data would be used, was considered as an example of what a deployment could look like if personal data would be used. The fulfilment of the general legal requirements was considered for this scenario. Overall, the legal requirements possibly could be passed in a final deployment. Some aspects which specifically should be considered are the withdrawal of consent, the amount of data received by the data processor and the data controller, how it will be ensured that the technology stays the state-of-the-art, how a privacy preserving logging can be achieved (including deletion when the data is not necessary anymore) and how the contractual relationships between the different actors will be shaped.

2. Document Information

2.1 Contributors

Name	Partner
Jessica Schroers	KUL
Pedro Malaquias	KUL
Hannah Obersteller	ULD

2.2 History

Version	Date	Author	Changes
0.1	1.10.2015	Jessica Schroers	
0.2	16.10.2015	Hannah Obersteller	
0.3	29.10.2015	Jessica Schroers	Version for review
1.0	30.10.2015	Jessica Schroers	Implemented reviewers comments

2.3 Table of Figures

2.4 Table of Acronyms

CI Credential Issuer

EEA European Economic Area

eIDAS Regulation (EU) 910/2014

IdP Identity Provider

LR Legal Requirement

PEPS Pan-European Proxy Service

SP Service Provider

2.5 Referenced Documents

FutureID deliverables

R. Robrahn, H. Obersteller, FutureID Deliverable 52.5 Legal aspects and evaluation of business and Cloud scenarios, version 1.0, 30.10.2015.

J. Schroers, N. Marnau, E. Schlehahn, B. van Alsenoy, 'FutureID Deliverable 22.6 Legal Requirements', v. 1.1., 11.12.2013.

Legislation

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, Official Journal L013, 19.1.2000 (eSignature Directive).

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Official Journal L257/73, 28.8.2014 (eIDAS Regulation).

Projects

epSOS: European Patients Smart Open Services, www.epsos.eu.

STORK: Secure Identity Across Borders Linked, www.eid-stork.eu and www.eid-stork2.eu .

3. Table of Contents

4. Project Description

The FutureID project builds a comprehensive, flexible, privacy-aware and ubiquitously usable identity management infrastructure for Europe, which integrates existing eID technology and trust infrastructures, emerging federated identity management services and modern credential technologies to provide a user-centric system for the trustworthy and accountable management of identity claims.

The FutureID infrastructure will provide great benefits to all stakeholders involved in the eID value chain. Users will benefit from the availability of a ubiquitously usable open source eID client that is capable of running on arbitrary desktop PCs, tablets and modern smart phones. FutureID will allow application and service providers to easily integrate their existing services with the FutureID infrastructure, providing them with the benefits from the strong security offered by eIDs without requiring them to make substantial investments.

This will enable service providers to offer this technology to users as an alternative to username/password based systems, providing them with a choice for a more trustworthy, usable and innovative technology. For existing and emerging trust service providers and card issuers FutureID will provide an integrative framework, which eases using their authentication and signature related products across Europe and beyond.

To demonstrate the applicability of the developed technologies and the feasibility of the overall approach FutureID will develop two pilot applications and is open for additional application services who want to use the innovative FutureID technology

Future ID is a three-year duration project funded by the European Commission Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 318424

5. Overall Evaluation Approach

The FutureID Evaluation approach uses a Design Science Methodology framework to organize and harmonize the multiple disciplinary evaluation approaches for all three artefacts: Reference Architecture, Implementation, and Pilots.

To provide a closer look, FutureID has simplified its evaluation process into three easy steps. First, we **identify** each of the artefacts: two pilots, a reference architecture, and implementation. Second, we **clarify** how each interdisciplinary team considers the artefacts and develop requirements regarding their disciplines. FutureID has interdisciplinary teams that cover the spectrum of important perspectives regarding: technical merit, security, privacy, usability, socio-economic, and legal. This step is ranked regarding importance and is done by using the Evaluation Wiki tool. Lastly, we **re-evaluate**, which means each requirement identified will be re-evaluated on whether they should be really implemented or initiated in each artefact. Of course, with the complexity of some of the artefacts an exhaustive evaluation could not be sufficiently executed with only this procedure. Therefore, extra evaluation steps were taken to properly consider specific needs of some of the artefacts.

The Evaluation Wiki tool is a quality control mechanism that has been used for the core evaluation of FutureIDs results. The Evaluation Wiki tool has a variety of different beneficial functions that lead to a practical and optimised evaluation method. On the practical side, it presents an easy to read, adjustable and comprehensive solution for documentation of the evaluation requirements needed for each artefact. Each artefact can be subcategorized into viewing each of the importance levels of requirements (must, should, may, not applicable) on the main page of the Evaluation Wiki tool. The Evaluation Wiki tool classifies each requirement, its origin (interdisciplinary team), its rank of importance, and includes a comment section.

While collaborating with multiple disciplines, harmonizing and consolidating a wide spectrum of requirements proved difficult and resulted in some conflicts. In order to solve this problem, FutureID included another addition to the Evaluation Wiki tool and to the Evaluation work package. The addition was another deliverable that focused on the clarification of which requirements are either similar to, relate to, or conflict with other requirements. This is a necessary task that all large scale interdisciplinary projects should have in order to harmonize evaluations' requirements. This task helped to provide insight on how all of the requirements can cooperate and be applied together.

In addition to these processes, the testbed has proven to be a great technical method for testing the implementation and pilot applications. It is built on three different levels of testing: unit testing, integration testing, and system testing. The implementation artefact is tested using the unit, integration, and system testing. While the pilots are tested only at the system level testing, the kind of evaluation methods between different artefacts obviously varies. However, the Design Science Evaluation methods are broad enough to cover a wide range of techniques.

6. Evaluation

The following tables include a comprehensive list of results regarding the legal requirements for each artefact (Reference Architecture, Implementation, and Pilots). The methodology explained above was applied in the evaluation of the legal requirements. In relation to each artefact, each requirement was analysed to determine the classification of importance, its test method, and the final result. In respect of the classification of importance, there are four possible outcomes: Must, May, Should, and Not Applicable.

The legal evaluation differs from the other evaluations, having its own particularities. First, each requirement was tested manually, as it is not possible to perform a legal evaluation automatically, using the testbeds described above. Second, a "must" classification was attributed to a large number of the requirements as they directly result from binding laws. On the other hand, a large number of requirements were classified as 'not applicable'.

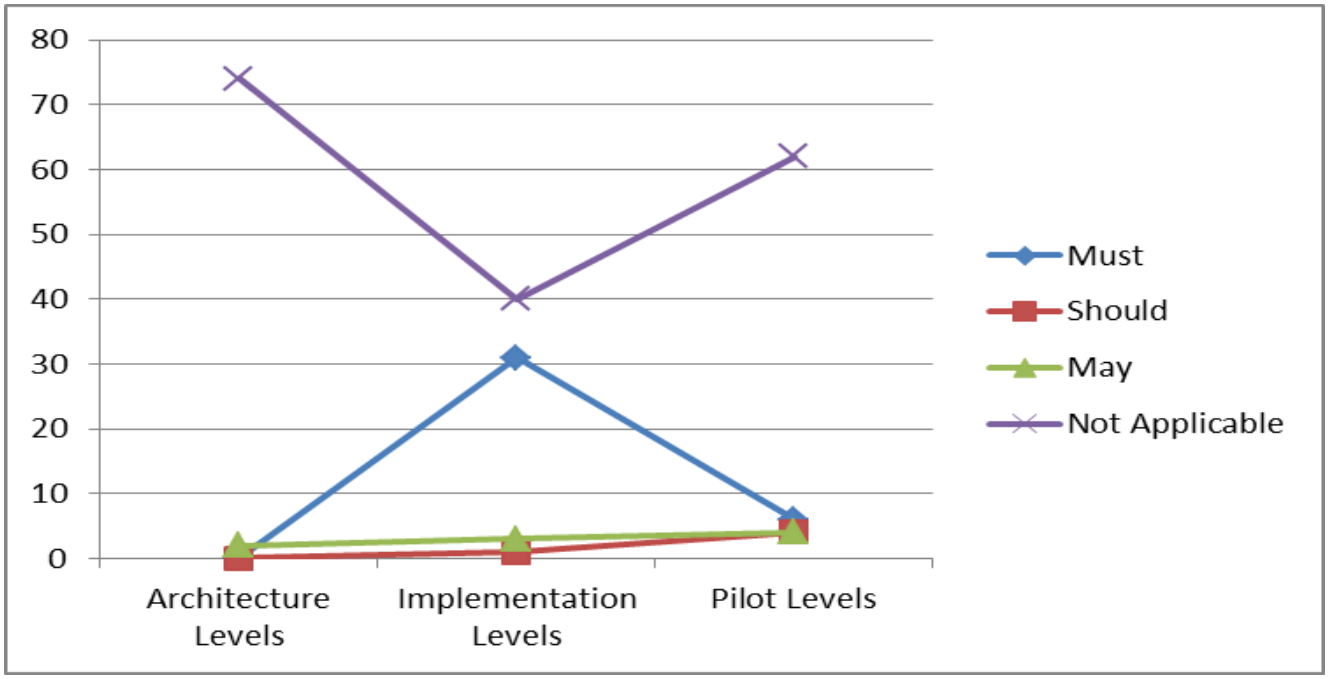

Figure 1 Graph of requirement level changes

There are several reasons for the attribution of a 'not applicable' classification to such a large number of requirements. First, due to the specific approach, many requirements entail IF clauses and are mutually exclusive (i.e., if one of the requirements is chosen, all the others become 'not applicable'). An example of this can be seen in Figure 2. The requirement LR-01.3 provides that a legal ground must be chosen within several possibilities. The application of one legal ground renders all the others (including their sub-requirements) 'not applicable'.

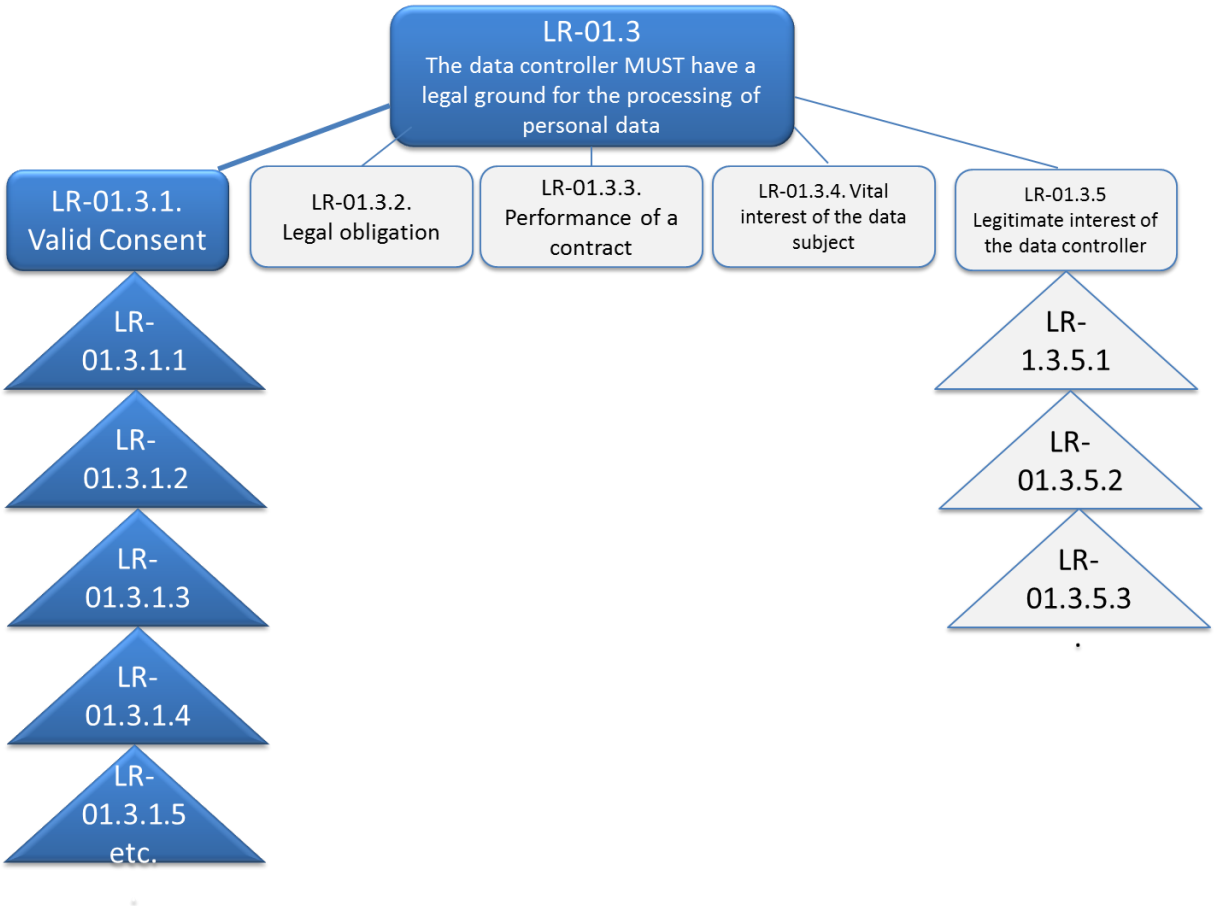

Figure 2 Mutually exclusive requirements

The second reason for the large number of 'not applicable' legal requirements results from the fact that they depend on the exact configuration of the final deployment. This leads to most requirements not being applicable to the '**Reference Architecture**' artefact. As for the '**Implementation**' artefact, there are some applicable requirements, which are assessed on the basis whether they facilitate the fulfilment of the requirements in the final deployment. Finally, the data protection requirements do not apply to the '**Pilots**' artefact, as the pilot applications do not process personal data. For this reason, a fourth section was added to this evaluation report, taking into account the final deployment. Naturally, at this point, it is not yet possible to evaluate the final deployment solution and attribute it a passed/failed classification. Instead, the pilots were assessed as if they would use personal data and a general overview and recommendations are provided to be taken into consideration for the final deployment.

The evaluation of the requirements has been performed manually. This was performed by conducting surveys and interviews with the responsible persons and evaluating the existing components (e.g. the user interface). In the following, for every artefact the applicable legal

requirements (LR) will be shown in tables. These include a description of the requirement, the classification on the applicable level, how it has been tested and the result of the evaluation.

6.1 Reference Architecture

The evaluation of the legal requirements depends on the exact configuration. Therefore, most requirements are not applicable to the Reference Architecture. We considered the two requirements that the FutureID infrastructure may provide the function to sign electronically and may make use of electronic certificates as passed, since the architecture considers the FutureID Client providing the functionality to sign electronically, and the use of electronic certificates.

LR-03.2	**Electronic signing**
Description	FutureID infrastructure MAY provide the function to sign electronically.
Classification on Architecture	May
How has it been tested?	Manually
Result	Passed

LR-03.3	Electronic certificates
Description	FutureID infrastructure MAY make use of electronic certificates.
Classification on Architecture	May
How has it been tested?	Manually
Result	Passed

6.2 Implementation

On the Implementation level, there are several important legal requirements. So that they are met, it is essential that the technical architecture allows for their execution in the final deployment.

As described previously and due to its specific nature, the general approach to the legal requirements is based on hierarchy levels, containing both joint and mutually exclusive requirements. This is especially visible in LR-01.3, which requires a legal ground for processing. The sub-requirements in LR-01.3 enumerate the different legal grounds for processing, including their sub-sub-requirements. In FutureID, the legal ground for processing is valid consent. Therefore, all the remaining requirements in respect of different legal grounds are rendered 'not applicable'.

In order to fulfil the 'valid consent' requirement, several sub-requirements need to be met. Only part of these can be analysed at the implementation level, as the fulfilment of several of them can only be analysed in the final deployment. Since the fulfilment of all the sub-requirements determines the fulfilment of the upper requirement, the passing of LR-01.3.1 depends on the passing of the sub-requirements. However, an overall pass of the high-level requirement can only be attributed if all sub-requirements are passed. Therefore, in the evaluation often only a provisional pass has been given for the specific level of evaluation, as at this point it is not yet possible to evaluate all the sub-requirements.

Furthermore, on the implementation level the fulfilment of requirements is considered differently from the other levels. On this level, passing simply means that technical means are provided to allow for, or facilitate the fulfilment of the requirement in the final deployment.

In the following, we go through all groups of legal requirements and explain selected aspects concerning sub-(sub-) requirements considered as especially relevant for the decisions made in the evaluation.

6.2.1 Legal ground for processing

For the evaluation of the LR-1.3 requirements, it has been assessed how the user gives consent for the authentication process. The user does give explicit consent since she is required to press a clearly identified button, while being informed that, by pressing it, she is giving consent and this will result in transfer of the specified data to the specified SP. As this information is given before any processing occurs and the client can provide all the necessary information to ensure that the user gives informed consent, the requirements are fulfilled. The withdrawal of consent is a requirement which refers to the fact that the user must be able to withdraw consent to processing at a later stage. The withdrawal is not retroactive, but it should prevent any further

processing of the data by the data controller.[1] As, in principle, this requirement can only be fulfilled by the data controller, for the implementation it has been analysed whether the user can get the information on who to approach in order to withdraw consent. As this information can be provided in the user interface, the requirement has been evaluated as passed on the implementation level.

LR-01.3	Legal ground for processing
Description	The data controller MUST have a legal ground for the processing of personal data (see D22.6 section 5.3.2 for further guidance).
Classification on Implementation	Must
How has it been tested?	Manually
Result	Passed

LR-01.3.1	Valid consent
Description	IF the legal ground for processing is the data subject's consent, the consent MUST be valid.
Classification on Implementation	Must
How has it been tested?	Manually
Result	Passed

LR-01.3.1.1	Unambiguity of consent
Description	The consent MUST be an unambiguous expression of the data subject's wishes.
Classification on Implementation	Must

[1] See D32.8 for more information.

How has it been tested?	Manually
Result	Passed

LR-01.3.1.2	Specific consent
Description	The consent expression MUST be distinctive and intelligible, referring clearly to the scope and consequences of data processing.
Classification on Implementation	Must
How has it been tested?	Manually
Result	Passed

LR-01.3.1.3	Informed consent
Description	The data subject's consent MUST be based on accurate, full and understandable information.
Classification on Implementation	Must
How has it been tested?	Manually
Result	Passed

LR-01.3.1.4	Freely given consent
Description	The consent MUST represent the data subject's genuinely free choice to allow the data processing activities.

Classification on Implementation	Must
How has it been tested?	Manually
Result	Passed

LR-01.3.1.4.1 (absence of pressure) and LR-01.3.1.4.2 (absence of relationship of dependence) are not considered on implementation level since it is not possible to ensure or even to facilitate this in a technical solution.

LR-01.3.1.5	Time to seek consent
Description	The consent MUST be asked for before any processing occurs.
Classification on Implementation	Must
How has it been tested?	Manually
Result	Passed

LR-01.3.1.6	Withdrawal of consent
Description	The data subject MUST be given the option to withdraw his or her consent and stop any further processing of the personal data.
Classification on Implementation	Must
How has it been tested?	Manually
Result	Passed

LR-01.3.1.7	Consent for sensitive data
Description	The data subject's consent for processing of sensitive data in the sense of Art. 8 95/46/EC MUST be explicit.

Classification on Implementation	Must
How has it been tested?	Manually
Result	Passed

6.2.2 Data quality requirements

The requirements with regard to data quality also refer to the obligations of the controller. Therefore, they can only be assessed in a limited scale at the implementation level. As previously, it has been assessed whether the implementation provides the possibility for the controller to comply with the requirements, and if the technical components do fulfil certain requirements. The requirement that the personal data must only be collected for specified, explicit and legitimate purposes is an example. This depends on the data controller. However, as the user interface is designed to show the purpose of the data processing, which means that the purpose will be specified and explicit, the requirement has been considered as passed. Similar is the assessment of LR-01.4.5. Regarding this requirement, it must be considered that the deletion of the data at the premises of the data controller cannot be assured within the implementation. However, it has been ensured that all the data that goes through the Broker Service will be deleted immediately after the process has been finished.

LR-01.4	Data quality
Description	The personal data and the processing MUST adhere to legal data quality standards).
Classification on Implementation	Must
How has it been tested?	Manually
Result	Passed

LR-01.4.1	**Fairness**
Description	Personal data MUST be processed fairly and lawfully.
Classification on Implementation	Must
How has it been tested?	Manually

Result	Passed

LR-01.4.2	**Purpose limitation**
Description	The personal data MUST only be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.
Classification on Implementation	Must
How has it been tested?	Manually
Result	Passed

LR-01.4.3	**Necessary and adequate for the purpose**
Description	The personal data MUST be adequate, relevant and not excessive in relation to the purposes for which it is collected and/or further processed.
Classification on Implementation	Must
How has it been tested?	Manually
Result	Passed

LR-01.4.4	**Accuracy**
Description	The responsible data controller MUST take every reasonable step to ensure that the personal data is accurate and up to date.
Classification on Implementation	Must
How has it been tested?	Manually
Result	Passed

LR-01.4.5	**Deletion**
Description	When no longer necessary for the purpose the personal data MUST be deleted or rendered anonymous.
Classification on Implementation	Must
How has it been tested?	Manually
Result	Passed

LR-01.4.5.1	**Secure deletion**
Description	The deleted personal data MUST NOT be retrievable.
Classification on Implementation	Must
How has it been tested?	Manually
Result	Passed

6.2.3 Data subject's rights

In principle, the passing of LR-01.5 requires that the sub-requirements LR-01.5.1 to LR-01.5.3 are passed. LR-01.5.1 (right to information) states that the data controller must provide the data subject with sufficient information. As the user interface provides the possibility to include this information, the requirement has been assessed as passed.

LR-01.5.2 and LR-01.5.3 (right to access and right to rectify) are considered as not applicable. In principle, they could be considered as passed, as the information in the user interface provides the possibility to indicate the controller and its contact information, which then can be used to enforce the user rights. However, as the safeguard of the right to access and the right to rectify is completely up to the Service Provider, and the provided information is a requirement of LR-01.5.1, the two sub-requirements have been considered as not applicable. The passing of LR-01.5 is therefore subject to the condition that the controller fulfils the sub-requirements LR-01.5.2 and LR-01.5.3.

LR-01.5	**Data subject's rights**
Description	The data controller (as well as the FutureID infrastructure and FutureID providers) MUST ensure the data subject's rights.
Classification on Implementation	Must
How has it been tested?	Manually
Result	Passed

LR-01.5.1	**Right to information**
Description	The data controller MUST provide the data subject with sufficient information, at least the identity of the controller, the categories of data to be processed, whether the information is obligatory or voluntary, the purpose for processing, the recipients of the data, and the further rights to access and to rectify.
Classification on Implementation	Must
How has it been tested?	Manually
Result	Passed

6.2.4 E-commerce requirements

The e-commerce requirements are applicable if the FutureID service/the Service Provider is an information society service (as recognisable from the IF clause). An information society service is any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a services' recipient. We assume that the FutureID provider will be either a separate FutureID Broker or a Service Provider, which would normally meet the requirements to be an information society service. Therefore, the requirements LR-02.2.1 to LR-2.2.7 must be fulfilled, and with them also LR-02.2. These requirements have been considered as passed on the implementation level, since the user interface provides the possibility to include the information.

LR-02.2.	Information society service
Description	IF the FutureID provider provides an information society service, it MUST fulfil the obligations of an information society service.
Classification on Implementation	Must
How has it been tested?	Manually → fulfilment of all LR-02.2. sub-requirements
Result	Passed

LR-02.2.1	Information society service – name
Description	IF the FutureID provider provides an information society service, it MUST provide its name.
Classification on Implementation	Must
How has it been tested?	Manually
Result	Passed

LR-02.2.2	Information society service - geographic address
Description	IF the FutureID provider provides an information society service, it MUST provide the geographic address at which it is established.
Classification on Implementation	Must
How has it been tested?	Manually
Result	Passed

LR-02.2.3	Information society service – contact details
Description	IF the FutureID provider provides an information society service, it MUST provide the contact details, including its e-mail address.
Classification on Implementation	Must
How has it been tested?	Manually
Result	Passed

LR-02.2.4	Information society service – trade registration
Description	IF the FutureID provider provides an information society service AND is registered in a trade or similar public register, it MUST provide the trade register and its registration number or equivalent means of identification in that register.
Classification on Implementation	Must
How has it been tested?	Manually
Result	Passed

LR-02.2.5	Information society service - authorization scheme
Description	IF the FutureID provider provides an information society service AND is subject to an authorization scheme, it MUST provide the particulars of the relevant supervisory authority.
Classification on Implementation	Must
How has it been tested?	Manually
Result	Passed

LR-02.2.6	Information society service - VAT number
Description	IF the FutureID provider provides an information society service AND its activity is subject to VAT, it MUST provide the VAT number.
Classification on Implementation	Must
How has it been tested?	Manually
Result	Passed

LR-02.2.7	Information society service - information access
Description	All the information required in LR-02.2 MUST be rendered easily, directly and permanently accessible to the recipients of the service.
Classification on Implementation	Must
How has it been tested?	Manually
Result	Passed

6.2.5 e-Signature requirements

The e-signature requirements are based on Directive 1999/93/EC. However, during the project, on 17 September 2014, Regulation (EU) 910/2014 (eIDAS Regulation) entered into force. Directive 1999/93/EC will be repealed as of 1 July 2016, while the provisions on electronic trust services (including e-signatures) of the eIDAS Regulation will applicable from that day. As a Regulation, the provisions of the eIDAS Regulation are directly applicable in the Member States and do not need to be implemented at national level. Therefore, the requirement "IF FutureID infrastructure provides the function to sign electronically it MUST adhere to the applicable national restrictions/requirements for electronic signatures" might become superfluous, as the Regulation is directly applicable. However, it is noteworthy to point out that national legislations are not invalidated following the entering into force of the eIDAS Regulation. The Regulation enjoys primacy in application, meaning that existing legislation contradictory to the Regulation will cease to be applicable once it enters into force. However, aspects that are not covered by the Regulation can still be covered by national law (as far as it does not contradict the European

provisions). For example, only trust services provided to the public having effects on third parties need to adhere to the eIDAS Regulations requirements. If the FutureID technology is used in a closed context, specific national requirements will remain applicable and need to be considered.

The requirements regarding the electronic certificates have been evaluated as passed, since, according to the provided information, the certificates used within the FutureID infrastructure do not entail restrictions.

LR-03.2	**Electronic signing**
Description	FutureID infrastructure MAY provide the function to sign electronically.
Classification on Implementation	May
How has it been tested?	Manually
Result	Passed

LR-03.2.1	**Electronic signing**
Description	IF FutureID infrastructure provides the function to sign electronically it MUST adhere to the applicable national restrictions/requirements for electronic signatures.
Classification on Implementation	Not applicable
How has it been tested?	Manually
Result	Passed

LR-03.3	electronic certificates
Description	FutureID infrastructure MAY make use of electronic certificates.
Classification on Implementation	May

How has it been tested?	Manually
Result	Passed

LR-03.3.1	**Restricted electronic certificates**
Description	IF the FutureID infrastructure uses electronic certificates with restrictions, it MUST use the electronic certificates within the borders of their eventual restrictions.
Classification on Implementation	Must
How has it been tested?	Manually
Result	Passed

LR-03.3.2	**Electronic certificates T&C**
Description	IF the FutureID infrastructure uses electronic certificates which are restricted by the terms & conditions of the certificate service provider, it MUST use the electronic certificates within these restrictions.
Classification on Implementation	Must
How has it been tested?	Manually
Result	Passed

LR-03.3.4	**Electronic certificates Member States**
Description	FutureID infrastructure MUST use electronic certificates within the borders of eventual restrictions set by Member States
Classification on Implementation	Must

How has it been tested?	Manually
Result	Passed

6.2.6 Other requirements for the implementation

These requirements have been evaluated as passed on the implementation level, based on the results of the technical and security evaluation, and the results of the interviews with the implementers. Possible logging depends on the configuration of the systems of the participants.

LR-01.6.	**Technical and organizational measures**
Description	Data controller and data processor MUST implement appropriate state-of-the-art technical and organizational measures to ensure security and confidentiality.
Classification on Implementation	Must
How has it been tested?	Manually
Result	Passed

LR-01.7.7	**Multi-tenancy**
Description	IF the data processor is acting on behalf of several different data controllers, the personal data of different controllers MUST support multi-tenancy, not combining or linking the data of different controllers.
Classification on Implementation	Must
How has it been tested?	Manually
Result	Passed

LR-04.2.3	**Evidence preservation**
Description	To be able to provide evidence in case of claims, technical or organizational measures SHOULD be possible, e.g. logging.
Classification on Implementation	Should
How has it been tested?	Manually
Result	Passed

6.3 Pilot(s)

Neither the 'Citizen Services pilot' nor the 'E-Learning Services for Enterprises pilot' make use of personal data. Therefore, the Requirements arising from the European Data Protection Directive do not apply. Likewise, as they are pilots, they do not provide information society services. Therefore, the Requirements arising from the E-commerce Directive are not applicable.

Thus, this section will only look at the e-signature requirements and the contract requirements that might be applicable. In case of e-signature requirements, the upper requirements are 'may' requirements, while the sub-requirements are 'must'. However, only if the 'may' requirements apply, the 'must' sub-requirements will need to be met.

The requirement that FutureID may provide the function to sign electronically is a top hierarchical requirement. In respect of the pilots, only for the Citizen Services pilot (WP 51) this requirement will be applicable in the signature use case. The only implication would be that the implementers, by fulfilling LR-03.2, must also fulfil LR-03.2.1. However, as explained in 6.2.6, this requirement will cease to be applicable following the introduction of the eIDAS Regulation, rendering it superfluous in the future. Still, the e-signature Directive and is national implementations shall remain applicable until 1 July 2016. As WP 51 also uses the Austrian qualified e-signature, requirement LR-03.1. is also considered as passed.

The requirements regarding contracts are in general 'should' requirements. The general legal relations between the project partners are regulated by the consortium agreement. However, if the project had conducted tests of the pilot applications involving real users and their personal data, a contract between the project partner(s) acting as data controller and the project partner(s) acting as the data processor would have had to be drafted, in order to provide a legal ground for the data processing and fulfilling the data protection requirements. Furthermore, Atos would have had to enter into an agreement with the Spanish PEPS to use the testing environment. As there are no real users in the pilots, there is no need for entering into a contract with them. Therefore, the requirements are considered as not applicable.

In respects regarding the liability requirements, which are also 'should' requirements, there are liability restrictions in section 5 of the consortium agreement. As no external service will be provided which could raise a liability risk, the requirement can also be considered as passed.

Finally, a pass has been attributed to the requirement regarding evidence in case of claims (LR-04.2.3), since it is possible to log the actions, which is sufficient for a 'should' requirement.

LR-03.1	**Electronic signatures**
Description	The FutureID infrastructure MAY make use of qualified electronic signatures
Classification on Pilot	May
How has it been tested?	Manually
Result	Passed

LR-03.2	**Electronic signing**
Description	FutureID infrastructure MAY provide the function to sign electronically.
Classification on Pilot	May
How has it been tested?	Manually
Result	Passed

LR-03.2.1	**Electronic signing**
Description	IF FutureID infrastructure provides the function to sign electronically it MUST adhere to the applicable national restrictions/requirements for electronic signatures.
Classification on Pilot	Must

How has it been tested?	Manually
Result	Passed

LR-03.3	**Electronic certificates**
Description	FutureID infrastructure MAY make use of electronic certificates.
Classification on Pilot	May
How has it been tested?	Manually
Result	Passed

LR-03.3.1	**Restricted electronic certificates**
Description	IF the FutureID infrastructure uses electronic certificates with restrictions, it MUST use the electronic certificates within the borders of their eventual restrictions.
Classification on Pilot	Must
How has it been tested?	Manually
Result	Passed

LR-03.3.2	**Electronic certificates T&C**
Description	IF the FutureID infrastructure uses electronic certificates which are restricted by the terms & conditions of the certificate service provider, it MUST use the electronic certificates within these restrictions.
Classification on Pilot	Must
How has it been tested?	Manually

Result	Passed

LR-03.3.3	**Electronic certificates liability limitation**
Description	The FutureID provider MUST be aware of eventual liability limitations of used electronic certificates.
Classification on Pilot	Must
How has it been tested?	Manually
Result	Passed

LR-03.3.4	**Electronic certificates Member States**
Description	FutureID infrastructure MUST use electronic certificates within the borders of eventual restrictions set by Member States
Classification on Pilot	Must
How has it been tested?	Manually
Result	Passed

LR-04.1	**Terms & Conditions/Contracts**
Description	FutureID provider SHOULD close contracts with related parties AND/OR provide terms & conditions they have to adhere to.
Classification on Pilot	Should
How has it been tested?	Manually
Result	Passed

LR-04.1.1	**Terms & Conditions of other parties**
Description	IF the terms & conditions of the other party apply to the FutureID provider, FutureID provider MUST follow the applicable Terms & Conditions of the other party OR FutureID provider MUST enter into specific contracts with the exclusion of the Terms & Conditions
Classification on Pilot	Must
How has it been tested?	Manually
Result	Passed

LR-04.2	**Liability**
Description	Liability depends on the national law. The FutureID provider SHOULD be aware of liability under the applicable law.
Classification on Pilot	Should
How has it been tested?	Manually
Result	Passed

LR-04.2.1	**Liability restrictions**
Description	FutureID provider SHOULD only state/guarantee the provisioning of functions which the system actually can provide
Classification on Pilot	Should
How has it been tested?	Manually
Result	Passed

LR-04.2.2	**Contractual liability restrictions**
Description	FutureID provider MAY restrict liability contractually to the extent legally allowed under the applicable law.
Classification on Pilot	May
How has it been tested?	Manually
Result	Passed

LR-04.2.3	**Evidence preservation**
Description	To be able to provide evidence in case of claims, technical or organizational measures SHOULD be possible, e.g. logging.
Classification on Pilot	Should
How has it been tested?	Manually
Result	Passed

6.4 Deployment

The exact terms of the final deployment cannot be assessed at this point. However, the legal requirements must be considered in the final deployment. To do this, a scenario where the pilots would be processing personal data will be considered. As the "e-Learning" pilot, developed in WP 52, provides a complete scenario, it is chosen as an example.[2] The analysis of the fulfilment of the requirements will be made accordingly.

The controller fulfils an essential role with regard to the legal requirements. In case of the pilot, Atos would be the controller and ECSEC GmbH (ECS) the processor. Therefore, Atos would be the party responsible to ensure the fulfilment of the legal requirements. LR-01.2 requires that for

[2] The "Citizen Services" pilot builds on an existing framework (epSOS) and improves its functionalities. The FutureID components cannot be assessed independently from epSOS. This is explained in detail in D51.5,

the FutureID use-cases the data controller must be resident of the EEA. This requirement would be fulfilled, as Atos is resident of Spain.

The requirements LR-01.7 to LR-01.7.7 detail the obligations with regard to the processor. In the case of the pilots, ECS would be the processor. The requirements would be fulfilled, as a controller-processor contract[3] was drafted in order to prepare a potential real user test, which takes into account all of the requirements aimed at the processor and the controller-processor relationship.

As neither Atos, nor ECS (whose servers are located in Germany) use foreign (sub-) processors for the FutureID data, the requirements LR-01.8 to LR-01.8.4 are not applicable. However, in a future deployment it is possible that processors from outside the EEA will be involved and will process personal data. In this case the requirements need to be considered.

The data controller would need to have a legal ground for processing the data. For Atos, this would be consent. In order to obtain valid consent, certain requirements need to be fulfilled. A consent form for Atos employees (and potential external participants) was drafted to prepare a real user test as well.[4]

The possibility of withdrawal of consent is a requirement which is often not considered by data controllers. Therefore, it is important that in the final deployment, the controllers implement strategies on how to react in case of a request to stop processing the data, and inform the data subject on how the controller can be contacted in case of withdrawal of consent. This information can be provided together with information on the general data subject rights. The FutureID User Interface is flexible and the easiest way to provide the required information would be via links. Here, information regarding the right to information, right to access and right to rectify must be provided, and the controller must have processes in place in order to answer to data subjects' requests and to inform other parties to whom the data has been possibly transferred.

The adherence to legal data quality standards can be provided jointly by implementation and by the controllers in a final deployment. As explained in the implementation section, the FutureID technology facilitates the adherence, e.g. by providing information on the purpose of the personal information that shall be transferred. However, this information is provided by the controller, which therefore has to ensure that the purpose of the data is specified, explicit and legitimate, and that the data will not be further processed in a way incompatible with this purpose. Furthermore, the data must be adequate, relevant and not excessive in relation to the purposes. In the case of the pilot this is questionable, as Atos requests all the content of an eID that is delivered by STORK. Although this data is not stored permanently, it is processed. If not

[3] The contract is provided as Annex I to D52.5.

[4] It is provided as Annex II to D52.5.

in any case, in some cases (especially with respect to non-Atos-employees) this approach can be considered justifiable. This aspect is discussed in detail in D52.5.

Under specific circumstances, the FutureID Broker might be obliged to ensure that only the minimum required data will be requested. For example, this might be an obligation in order to receive a German nPA certificate.

Within the scope of the information provision, the requirements regarding information society services also need to be considered. As mentioned in the implementation section, an information society service is any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. The SP will likely be an information society service provider, and will provide the required information at their website. However, if the FutureID service provider is a separate legal entity, as soon as it provides the service for remuneration (this could also include showing commercials in the user interface) it needs to provide the required information to the user.

The requirement that the data controller must take every reasonable step to ensure that the personal data is accurate and up to date will normally be fulfilled by the fact that trustworthy IdPs will be used to provide the information. The information itself will generally come from the CI/IdP and can therefore be corrected only at these entities. Considering this, it might be useful for an improved version of FutureID to show the user the exact information that will be sent, instead of only ‘name’ or ‘e-identifier’. This would allow the user to react immediately and contact the IdP if the information is no longer accurate. This is however outside of the scope of the FutureID project.

The data controller must ensure that the personal data will be deleted or rendered anonymous when it is no longer necessary for the purpose. Atos is not only obliged do this at their premises, but as ECS is the processor, the controller as the responsible parties must ensure that ECS will delete the information once it is no longer necessary. In principle the FutureID technology has been designed in a way that the information in the Broker Service will not store data and therefore the data will be deleted immediately following the authentication.

According to the information of developers and security reviewers, appropriate state-of-the-art technical measures are implemented. In case of a deployment, organizational measures to ensure security and confidentiality of the personal data must be implemented by the data controller and data processor. With regard to the pilot, this is fulfilled. However, in a final deployment scenario and considering that the technology will be provided open source, it needs to be clarified how it will be ensured that the technology will be kept state-of-the-art.

A difficult issue is to provide evidence in case of claims. Logging, for example, would be required. This might be in conflict/stretch privacy requirements such as that information should be deleted as soon as it is not needed anymore. It should in general be avoided to log personal information and preference should be given to log information on the functioning of the system

without personal information. Technically the logging depends on the configuration and can be decided by each participant on their system level.

Finally, the requirements cover contracts and liability. In this regard it will be important that the FutureID Broker will confirm with the IdPs that it can use their service. Furthermore, the FutureID Broker should enter into contracts with all involved parties, and consider liability risks and how and by which party they can be addressed.

7. Conclusion

We have evaluated the three artefacts on the basis of the legal requirements of D22.6. Overall, the general evaluation approach had limited usability for the legal requirements. In general, the majority of the legal requirements were not applicable for the three artefacts. However, it was still useful to divide the evaluation on the three artefacts. For a future evaluation it might be useful to consider the evaluation approach already during the formulation of the requirements and consider different requirements which could be applicable for each artefact. For the reference architecture almost no requirements were applicable, but it might be possible in future projects to formulate some general privacy preservation requirements (however, within FutureID this was already covered in the privacy requirement/evaluation task) which could also be applicable to the architecture.

With regard to the implementation artefact, some requirements were applicable, and all applicable requirements have been considered as passed since the implementation allows a legally compliant deployment. However, it would often still depend on the factual implementation. For instance, the implementation does allow that data is immediately deleted after it is not used anymore. Therefore, the requirement has been evaluated as passed for the implementation artefact. However, in general it is also possible to retain data, therefore the passing of a requirement on an implementation level does not automatically mean legal compliance of the deployment. Accordingly, for an evaluation whether a system is legally compliant, the final deployment is the important part, which could however (which is a common difficulty in research projects) not be assessed, as the final deployment is not yet realized. For this reason, and due to the fact that most requirements for the pilots were not applicable as no personal data is used, we used the e-learning pilot as an example of what a deployment could look like if personal data would be used, and assessed the requirements in general against this scenario. Overall, the legal requirements possibly could be passed in a final deployment. One aspect which could not be considered due to a lack of information is the withdrawal of consent, which needs to be implemented by the data controller. A point which should be taken into account is the amount of data received by the data processor and the data controller, which depends on the exact eID means used. However, the FutureID approach already employs a stronger data minimisation compared to other authentication systems, therefore it will often depend on the exact requests of the data controller. Further points which need to be taken into account in a deployment are how

it will be ensured that the technology stays the state-of-the-art, how a privacy preserving logging can be achieved, including deletion when the data is not necessary anymore, and how the contractual relationships between the different actors will be shaped.